

**Phil Keown**  
Engagement Lead  
T: 020 7728 2394  
E: philip.r.keown@uk.gt.com

**Will Simpson**  
Associate Director  
T: 0161 953 6486  
E: will.g.simpson@uk.gt.com

**Robert Jebbett**  
Executive  
T: 0161 953 6346  
E: robert.jebbett@uk.gt.com

## Information Commissioner's Office

### Internal Audit 2015-16: Core Operations (Post Eagle)

Last updated 5 July 2016

Distribution		Timetable	
For action	Paul Arnold – Head of Customer and Business Services	Fieldwork completed	29 February 2016
	Andy Laing – Head of Business Improvement	Draft report issued	9 May 2016
For information	Senior Corporate Governance Manager	Management comments	25 May 2016
	Audit Committee	Final report issued	26 May 2016

# Contents

## Sections

<b>1</b>	<b>Executive Summary</b>
<b>2</b>	<b>Detailed findings</b>

## Appendices

<b>A</b>	<b>All questions and detailed stakeholder responses</b>	<b>10</b>
<b>B</b>	<b>Internal Audit Approach</b>	<b>24</b>

## Glossary

<b>1</b>	The following terms are used in this report:
<b>4</b>	ICO – Information Commissioner's Office

This report is confidential and is intended for use by the management and Directors of the ICO only. It forms part of our continuing dialogue with you. It should not be made available, in whole or in part, to any third party without our prior written consent. We do not accept responsibility for any reliance that third parties may place upon this report. Any third party relying on this report does so entirely at its own risk. We accept no liability to any third party for any loss or damage suffered or costs incurred, arising out of or in connection with the use of this report, however such loss or damage is caused.

It is the responsibility solely of the ICO management to ensure that there are adequate arrangements in place in relation to risk management, governance and control.

# 1 Executive Summary

## 1.1 Background

The 2015-16 Internal Audit plan included a review of core operations, in particular how the ICO handles enquiries, written concerns and complaints from the general public and organisations.

In December 2013, the ICO announced its intention to review and change its approach in dealing with complaints and concerns to provide assurance that its work was focused on improving information rights practice in a manner that demonstrated clear value for money. To support these changes, the ICO published a consultation document inviting comment from stakeholders who represented the interests of data subjects or data controllers (business subject to the DPA) to understand the potential impact of the changes on:

- addressing complaints and engaging with businesses;
- quantifying the change in the burden of the ICO's activity on businesses;
- to receive suggestions on how any changes in burden could be minimised or decreased further; and
- to gauge opinion on the proposal to publish the number of concerns raised with the ICO about each organisation.

Following the implementation of operational changes made as part of Project Eagle, we have revisited the results of the 2013-14 ICO consultation entitled "Our new approach to data protection concerns" and conducted a survey of stakeholders to evaluate the impact of the changes made.

In undertaking our review, we:

- Engaged with the respondents to the original consultation document (using a questionnaire agreed with the ICO) to understand what impact the operational changes have had on their organisations (if any), and how the ICO has worked with them to improve their information rights practices since implementation;
- Contacted a further sample of organisations with which the ICO has engaged (from a complaint, regulatory action or voluntary review) to understand the effectiveness of the engagement, again using a questionnaire agreed with the ICO;
- Confirmed that the ICO published information by organisation and sector relating to concerns received together with consultation documents and legislative guides that align with Corporate Plan deliverables and the changing external environment.

## 1.2 Overall summary of results

### Organisational size and engagement type

In summary, over 80% (13 of the 15) of respondents were from "large" organisations (i.e. categorised as having over 2,000 employees) and over 93% of respondents were "experienced in the area of data processing" (answering 'over 10 years' when asked the question of how long they have been a data controller).

Answers to the question "what have been the reasons for your organisation's engagement with the ICO" found that the ICO engages in ways other than in the investigation of data subject complaints in 50% of cases. As would be expected due to the size of the organisations who responded, all had been the subject of an investigation or required assistance due to data subject complaints and 30% had submitted themselves for voluntary review; guidance had been provided in only 50% of cases.

As data security failures are more widely reported upon in the media and the public more educated in respect of their information rights, it becomes even more important that the ICO proactively promotes the guidance that is available to key stakeholders, rather than awaiting specific requests.

### Resource impact seen by organisations following changes in ICO engagement

When specifically questioned if the changes in the manner in which the ICO engaged with data subjects and the organisations had impacted the resource required to deal with engagements, 80% of respondents answered that it had not, with the remaining 20% of organisations reporting the impact to be approximately one additional member of staff.

A comment was received from one respondent in relation to the inconsistency of target response dates requested from caseworkers which had varied from 7 to 28 days.

The ICO should therefore look to provide greater clarity when communicating target response dates and give reasons for variations in response times. We would expect consistency in target response dates for the same type of request (e.g. new cases or investigations and further information requests) which are realistic and applied across all ICO departments.

### ICO responsiveness and effectiveness of recommendations

73% of respondents found the ICO to be "responsive to discussion and flexible in its approach" In the cases where organisation responded otherwise it was noted that:

- Investigations may be extremely prolonged (up to twelve months);
- Contact is made by the ICO via more than one route, despite requesting a single point of contact;
- Response times requested by the ICO are often unachievable given the organisation's size and complexity;
- The ICO has been slow to respond and appeared defensive when challenged on decisions.

In addition, of the 14 organisations who had received ICO recommendations on improving the management of data, it was commented that:

- "the majority or all of the recommendations were appropriate" in 43% of cases,
- "most...were appropriate" in an additional 43%.
- In the other 14% of cases, the organisations provided further detail to their answer, in one case noting that "recommendations made were already in place when made" and in the other, "were based on conclusions that were reached without clarifying the full facts of the case, or did not add sufficient value by identifying the root cause of the issue". One respondent noted that recommendations made following investigations were generally to "review our processes and see if we could have done something different".

We understand that the ICO maintains a casework quality review programme that feeds into staff performance management and development. To support this process, we would also expect that the ICO increases the transparency around recommendation development by including the rationale (for example, documenting the risk and impact of not complying) for each action.

Detailed findings and recommendations are provided in Section 2.

A complete summary of all stakeholder responses has been collated and is presented at Appendix A.

### **Publishing statistics on the volume of data concerns received**

When questioned on their views on the publishing of statistics relating to information subject complaints, respondents were also divided in their opinions. Whilst 75% agree that the information should be published, they would like to see changes in the format, with respondents noting that, *"it is important that appropriate context is provided"*, as specifically:

- The number of concerns raised is not necessarily an indicator of non-compliance;
- Statistics do not take into account the size of the organisation, and therefore the number of data subjects about whom personal data is processed;
- The published numbers also do not take into account the number of cases where the ICO finds in the favour of the Data Controller.

From April 2016, management confirmed that the ICO is to change the manner in which it presents this data. The ICO will publish only raw complaints data. For example, the ICO has confirmed that it intends to proactively disclose raw data, with a very small number of exceptions, about each complaint and self-reported incident it deals with. This report is to be published at the end of each month and relate to cases closed three months earlier. This gives time for a case to be appealed or be reviewed following its original closure before details about it are disclosed.

The ICO does not plan to collate this raw data into any league tables or reports. Readers are therefore free to interpret the data without any influence from the ICO

## 2 Detailed findings

### 1. Stakeholder engagement

Observation	Consideration for action	Agreed action (Date / Ownership)
<p>Responses to question 3, "<i>what have been the reasons for your organisation's engagement with the ICO</i>", found that all respondents had been the subject of an ICO investigation or required assistance from the ICO due to data subject complaints. This is as would be expected due to the size of the organisations who responded,</p> <p>30% of respondents had submitted themselves for voluntary review, but guidance had been provided in only 50% of cases.</p> <p>As data security failures become more widely reported upon in the media, and the public become more educated in their information rights, there is a risk that data owners or data processors may not manage their engagement either correctly or in the most effective manner, increasing the number of complaints made to the ICO.</p>	<p>The ICO should consider if there is any value in proactively promoting the available guidance, including the development of timetables for the publishing of new or updated guidance.</p> <p>They should also consider position statements about how guidance may be utilised most effectively by organisations.</p>	<p>Action agreed and implemented. Timetables are being drawn up for drafting new (and amending existing) guidance relating to the EU data protection reforms. There will also be guidance on the steps data controllers need to take to make best use of the guidance.</p> <p>Owner: Steve Wood Head of Policy Delivery</p>

## 2. Consistent response timescales

Observation	Consideration for action	Agreed action (Date / Ownership)
<p>When asked if changes to engagement methods <i>"had increased the resource impact on the organisation"</i> (Question 5), one respondent commented that response target dates set by caseworkers varied from 7 to 28 days with no underlying or consistent rationale being provided for the differing timescales. Management informed us that response timescales are dependent upon the circumstances of the individual case, including factors such as how long the case has been 'live' or whether the organisation has already had the opportunity to collate information about the case or respond to the complainant.</p> <p>By not effectively communicating the rationale behind response target dates or by not applying consistent target response dates across categories of cases, there is a risk that external organisations are not able to respond to engagements in an effective manner, or may incur additional costs in meeting target dates that are unrealistic, ultimately impacting upon their reputation or that of the ICO.</p>	<p>When setting target response dates for new cases, the ICO should aim to be transparent in explaining what was required from stakeholders and explain why particular timescales have been set when entering into any correspondence.</p> <p>This is in addition to the need for responses to be consistent in cases that display similar factors.</p>	<p>Action agreed</p> <p>Date Effective: 31 August 2016</p> <p>Owner: Andrew Laing Head of Performance Improvement</p>

### 3. Casework quality management

Observation	Consideration for action	Agreed action (Date / Ownership)
<p>In answer to questions 13 and 14, <i>"How responsive have you found the ICO to questions or concerns in relation to its service or approach?"</i>, 73% of respondents found the ICO to be <i>"responsive to discussion and flexible in its approach"</i>.</p> <p>In the cases where organisation responded otherwise it was noted that:</p> <ul style="list-style-type: none"> <li>Investigations may be extremely prolonged (up to 12 months);</li> <li>Organisations often have to deal with several caseworkers which was commented on as potentially causing additional work for the customer, despite them requesting a single point of contact; and</li> <li>The ICO has been slow to respond and appeared defensive when challenged on decisions.</li> </ul> <p>In addition, of the 14 organisations where the ICO had made recommendations to improve the management of data, in 21% of cases, the respondents noted that improvements could be made regarding the advice given, commenting that:</p> <ul style="list-style-type: none"> <li><i>"Recommendations made were already in place when made"</i>;</li> <li><i>"[Recommendations] were based on conclusions that were reached without clarifying the full facts of the case, or did not add sufficient value by identifying the root cause of the issue"</i>; and</li> <li>Recommendations made following investigations were generally to <i>"review our processes and see if we could have done something different"</i>.</li> </ul> <p>Management informed us that there is already a quality review process in place for casework, feeding into the performance management and staff development process,</p>	<p>The ICO should provide clear reasoning behind the recommendations that it makes to organisations.</p> <p>This is to provide assurance that the recommendations are proportional, add value and mitigate the issues arising.</p>	<p>Action agreed</p> <p>Date Effective: 31 August 2016</p> <p>Owner: Andrew Laing</p>



### 3. Casework quality management

Observation	Consideration for action	Agreed action (Date / Ownership)
which considers investigation completion, quality and proportionality of recommendations and quality of correspondence. However, in not completing reviews in a timely manner or by making recommendations that fail to address data management control weaknesses or add value to stakeholder organisations, there is a risk of reputational damage to the ICO, which may reduce the number of voluntary submissions or requests for advice, guidance and training.		

#### 4. Publishing complaint statistics

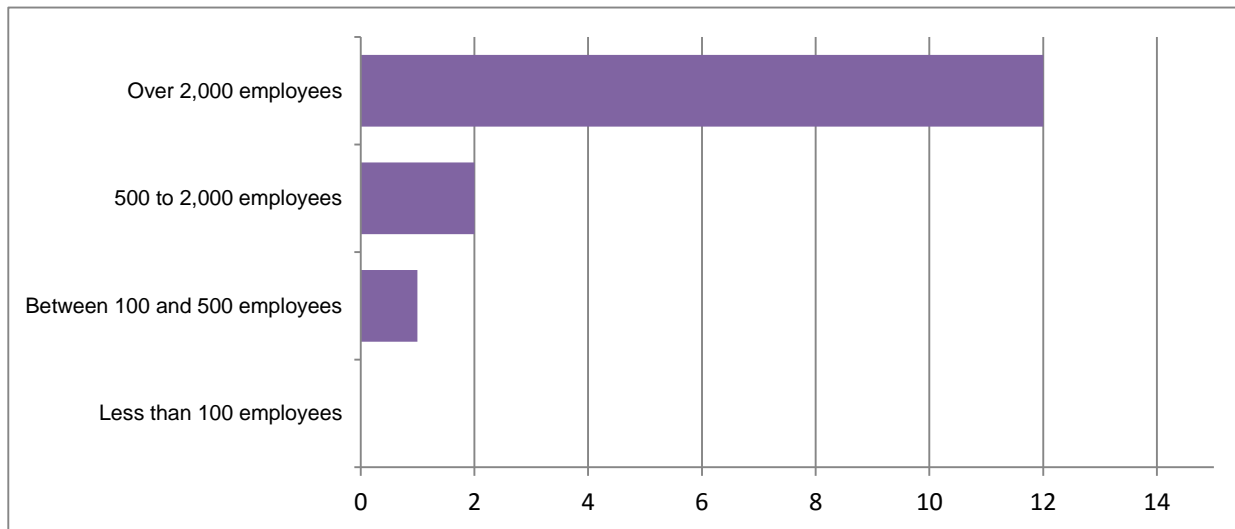
Observation	Consideration for action	Agreed action (Date / Ownership)
<p>Stakeholders were specifically questioned on their views on the publishing of statistics related to information subject complaints. Whilst 75% of the respondents agree that the information should be published, comments received noted that they would like to see changes in the format, including:</p> <ul style="list-style-type: none"> <li>• "it is important that appropriate context is provided"</li> <li>• "The number of concerns raised is not necessarily an indicator of non-compliance";</li> <li>• "Statistics do not take into account the size of the organisation, and therefore the number of data subjects about whom personal data is processed";</li> <li>• "Published numbers also do not take into account the number of cases where the ICO finds in the favour of the Data Controller".</li> </ul> <p>There is a risk that, by failing to effectively review data collated and the manner in which it is presented, statistics on information subject complaints do not reflect the current maturity of stakeholder organisation's data management controls or take into account organisational size or current relationship with their customers or the general public.</p>	<p>The ICO should review the format and contents of the information published on the volume of data concerns received, taking into account organisational size and where the organisation has not been found to be at fault.</p>	<p><i>The ICO has already reviewed the format and content of the information it publishes on the volume of data concerns received.</i></p> <p><i>We appreciate that organisations are not keen for us to publish information about the number of complaints received about them, particularly where the outcome did not result in a breach of any legislation. However, integral to Project Eagle was the belief that organisations could, and should, do more to explain their processing of personal information to their customers and stakeholders. We believed that if this happened then fewer people would be confused and feel the need to complain to the ICO unnecessarily. Evidence since the implementation of Project Eagle supports this view with many large organisations seeing a reduction in the number of complaints where no breach of the legislation is recorded. We therefore intend to continue to include all complaints we receive, not just those where a negative outcome for the organisation is reached.</i></p> <p><i>We also appreciate that large organisations feel penalised when our casework statistics are placed into a league table. We understand this concern. We do however believe that readers of our statistics are likely to take automatic account of the size of each organisation so as not to compare a major bank with a small limited company. However, comparisons between two well-known major banks would seem fair.</i></p>

#### 4. Publishing complaint statistics

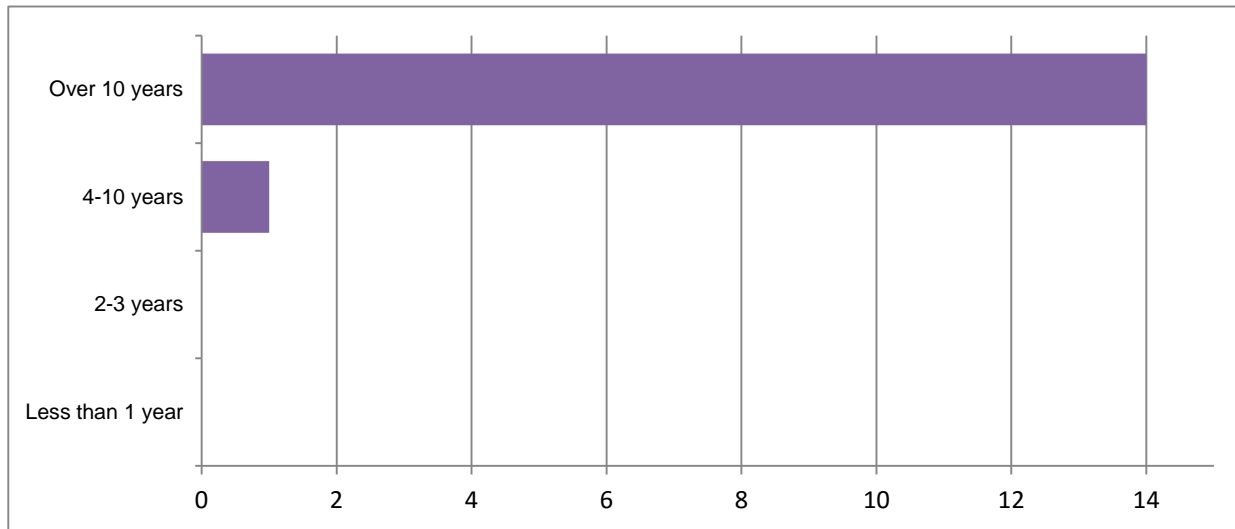
Observation	Consideration for action	Agreed action (Date / Ownership)
		<p><i>Notwithstanding this we have decided to stop publishing figures in league tables or with any form of ICO analysis applied. We are instead about to start publishing raw data reports which just show each complaint or self-reported incident reported to us, the organisation involved, the outcome, the nature of the issues dealt with and the relevant dates. This information will be published in reusable form so others may choose to compile reports based on it, but as a regulator we will simply be being transparent about the work we have received and its outcome. If we do not proactively disclose this information we will be asked to disclose it under FoI and will be obliged to do so. We currently receive approximately 3 requests per week for various sub sets of this information. The question is not therefore whether or not we publish it, but how we do it. We are choosing to do it proactively but without interpreting the data.</i></p> <p><i>Date Effective: 30 June 2016</i></p> <p><i>Owner: Paul Arnold</i></p>

## A All questions and detailed stakeholder responses

### Q1. How large is your organisation?

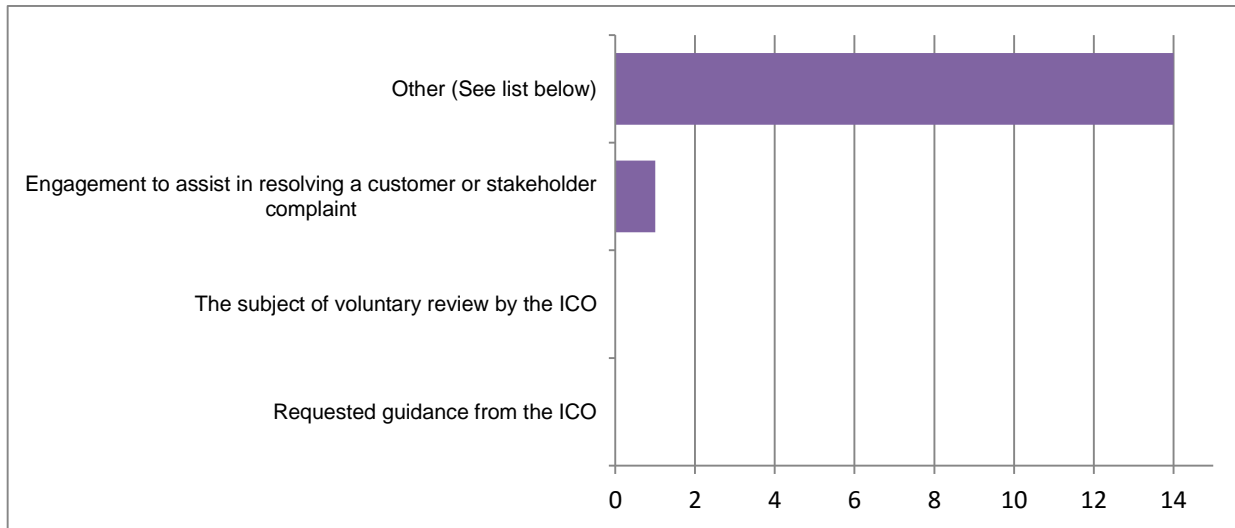


Answer Choices	Responses	
Less than 100 employees	0	0.00%
Between 100 and 500 employees	1	6.67%
500 to 2,000 employees	2	13.33%
Over 2,000 employees	12	80%
Total	15	100%

**Q2 How long has your organisation been a data controller / data processor?**

Answer Choices	Responses	
Less than 1 year	0	0.00%
2-3 years	0	0.00%
4-10 years	1	6.67%
Over 10 years	14	93.33%
Total	15	100%

### Q3 In this time, what have been the reasons for your organisation's engagement with the ICO?



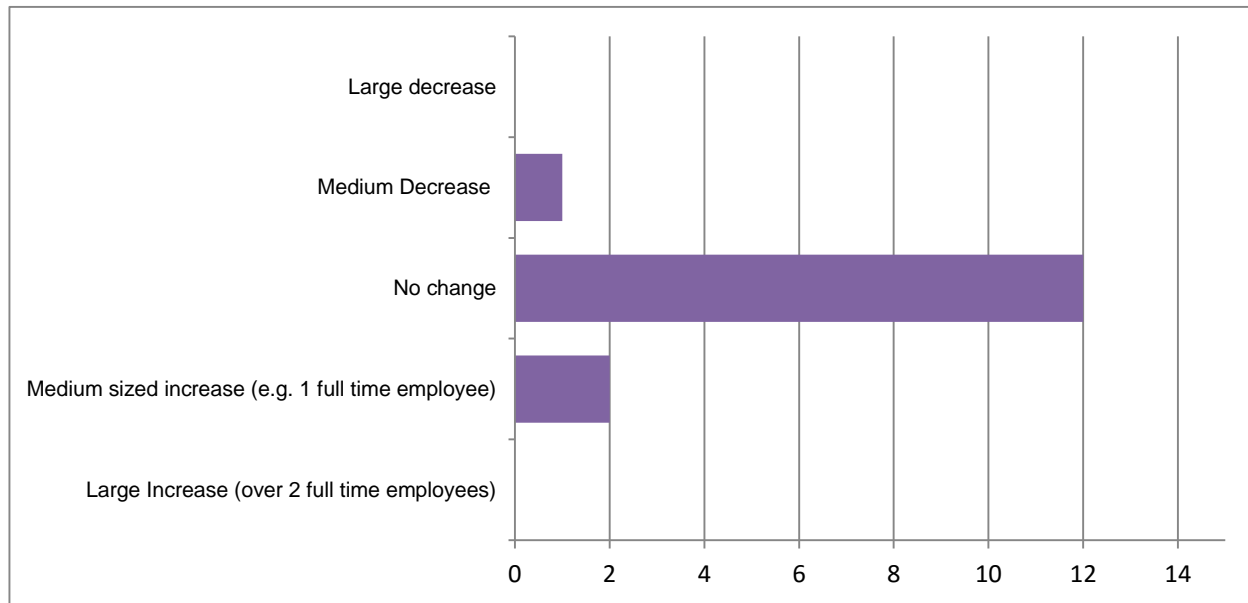
Answer Choices	Responses	
Requested guidance from the ICO	0	0.00%
The subject of voluntary review by the ICO	0	0.00%
Engagement to assist in resolving a customer or stakeholder complaint	1	6.67%
Other (See list below)	14	93.33%
<b>Total</b>	<b>15</b>	<b>100%</b>

---

**Q3 (continued) In this time, what have been the reasons for your organisation's engagement with the ICO?****Detailed Responses**

- Four respondents answered "All of the above".
- "Responding to complaints sent to the ICO".
- "Resolving complaints, requesting guidance and input into specific issues e.g. SARs relating to PPI/bank charges."
- "Requested guidance, Regular investigation of customer complaints, Performance monitoring of FOI and SAR cases. "
- "An Information Risk review of Credit Reference Agencies (July 2104). Also individual contacts relating to data subject complaints received by the ICO."
- "All of the above and providing training and investigating incidents."

#### Q4 Has the change in the method of engagement by the ICO impacted your company?



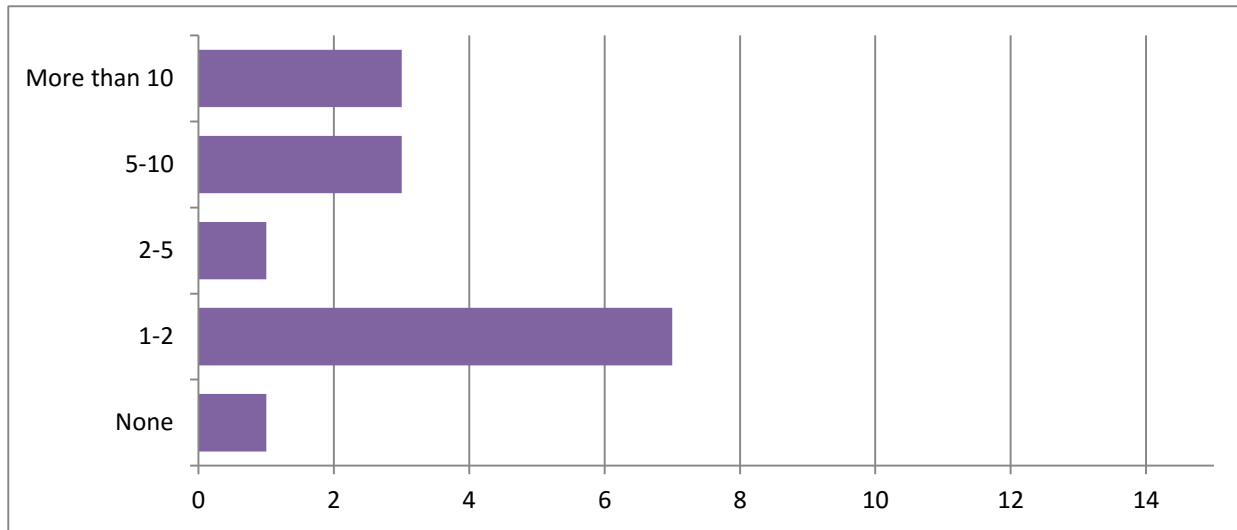
Answer Choices	Responses	
Large Increase (over 2 full time employees)	0	0%
Medium sized increase (e.g. 1 full time employee)	2	13.33%
No change	12	80.00%
Medium Decrease	1	6.67%
Large decrease	0	0.00%
<b>Total</b>	<b>15</b>	<b>100%</b>



---

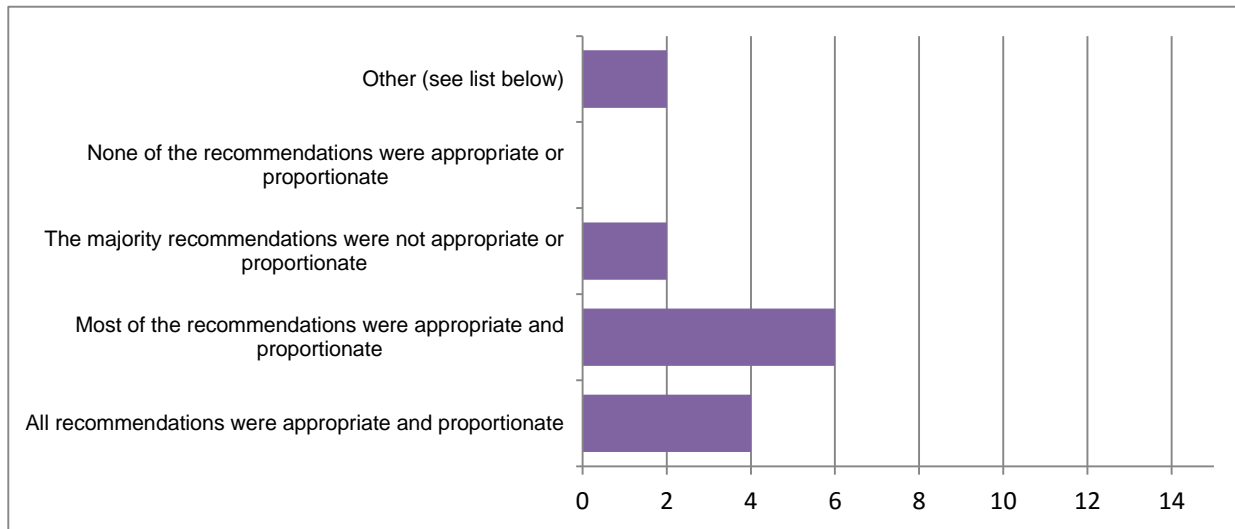
**Q5 If you have seen an increase in resource requirement, are you able to suggest steps to decrease this impact in the future?****Detailed responses**

- “Case officer training to ensure that complaints are valid before escalation.”
- “More consistency in communication from case officers. “
- “One point of contact for the ICO to use. Currently we receive communications via a number of officers and email addresses.”
- “Whilst we have not taken on additional employees we have still been affected by the changes. Historically all new requests for information about a consumer had a response timeframe of 28 days, over the last 12-18 months this has changed and random response times have been requested. When challenged I was informed that the 28 days were not a specified timeframe and it is up to each individual case worker to determine how long they feel is appropriate to respond (in the 10 years of dealing with the ICO the response times have always been 28 days for new investigation and 14 days for further information). Now (with no change) this can be as little as 7 days for a new investigation. Whilst it may seem as though the request is small in size to the ICO, the investigation internally may involve a number of departments to explain the process of events.”

**Q6 Has the ICO made suggestions or recommendations to your organisation in the last eighteen months?**

Answer Choices	Responses	
None	1	6.67%
1-2	7	46.67%
2-5	1	6.67%
5-10	3	20.00%
More than 10	3	20.00%
Total	15	100%

**Q7 Would you consider these suggestions or recommendations effective, appropriate and proportionate to the risks or issues identified?**



Answer Choices	Responses	
All recommendations were appropriate and proportionate	4	28.57%
Most of the recommendations were appropriate and proportionate	6	42.86%
The majority recommendations were not appropriate or proportionate	2	14.29%
None of the recommendations were appropriate or proportionate	0	0.00%
Other (see list below)	2	14.29%
<b>Total</b>	<b>14</b>	<b>100%</b>

---

**Q7 (continued): Would you consider these suggestions or recommendations effective, appropriate and proportionate to the risks or issues identified?**

**Other (detailed responses)**

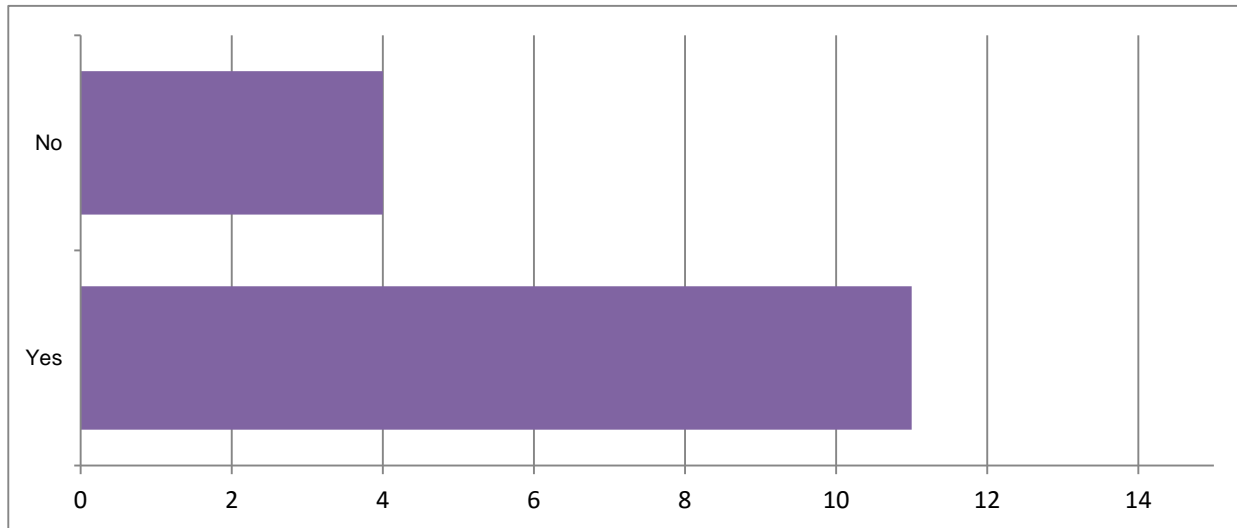
- “There have been cases where the ICO has made an assessment without seeking our explanation of events or fully understanding what has actually happened - but has deemed us to be in the wrong based solely on the concern/complaint received by them.”
- “Most were appropriate and proportionate but in many cases had already occurred or were in already in place.”

**Q8 If you found that the majority of suggestions or recommendations were not appropriate or proportionate, can you provide a reason why not?**

**Detailed response**

- “Recommendations are generally to *‘review our processes and see if we could have done something different’*.”

**Q9 Do you agree with the ICO publishing the number of data protection and information rights concerns raised during the year?**



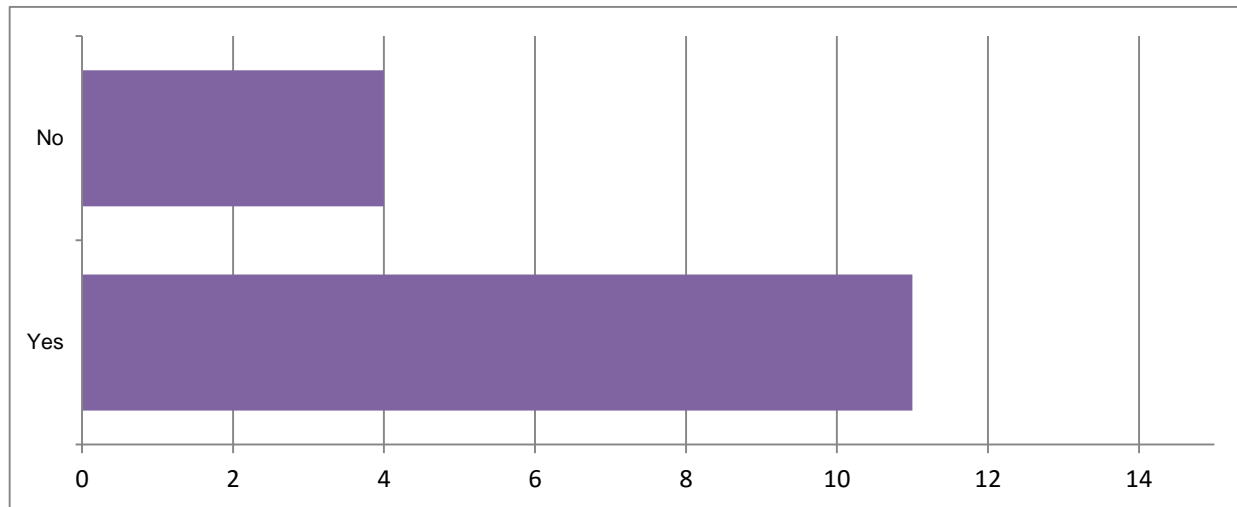
Answer Choices	Responses	
Yes	11	73.33%
No	4	26.67%
Total	15	100%

---

**Q10 If 'No', can you provide a reason why not?****Detailed responses**

- “Although I don't have a problem with the publishing of the number of concerns, it is important that appropriate context is provided.”
- “Some complaints are not valid and showing just the number can be misleading.”
- “Agree with ICO publishing numbers they receive but not the numbers relating to different organisations. The number of concerns raised is not a [sic] indicator of non-compliance. Just because a complaint/concern is raised does not necessarily mean that a controller or processor has done anything wrong.”
- “Concerns may be raised for spurious reasons and may not indicate any mishandling of data by the data controller. A simple figure of number of concerns raised does not provide any useful information on how well the data controller handles personal information.”
- “Stats are very misleading for larger organisations because they fail to take into account the number of data subjects about who personal data are processed. In addition, the published numbers do not take into account the number of cases where the ICO finds in the favour of the Data Controller. In something like 40+% of the complaints we get, the ICO finds there has been no breach committed. Publishing figures bases purely on cases received is simply wrong.”

**Q11 Do you agree with the ICO identifying the organisations about whom data protection and information rights concerns have been raised?**



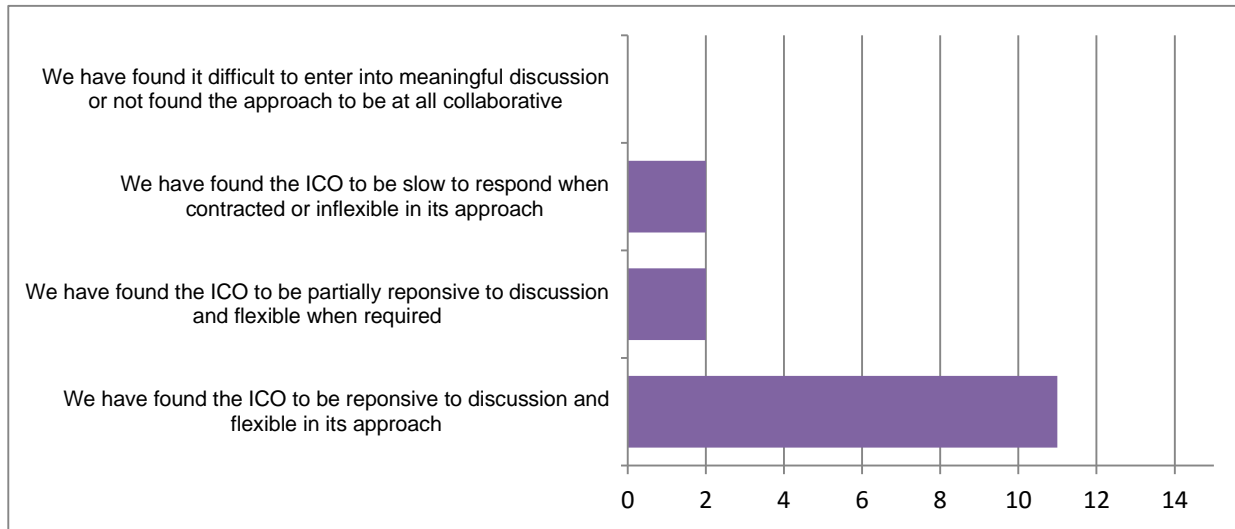
Answer Choices	Responses	
Yes	11	73.33%
No	4	26.67%
Total	15	100%

**Q12 If no, can you provide a reason why not?**

**Detailed Responses**

- “As per the previous question, it is important that context is given.”
- “Some complaints are not valid and showing just the number can be misleading.”
- “As per the previous question - the fact that a concern has been raised does not mean that an organisation has necessarily done anything wrong. There could be unfair damage to organisations' reputations.”
- “We agree with identifying the organisations only if complaints found to be invalid or of a 'spurious' nature are not included. Otherwise no.”
- “It would be much better to publish by sector that pin point specific organisations. In almost all cases, the largest Data Controllers will always receive the most complaints. In our opinion this is misleading.”

### Q13 How responsive have you found the ICO to questions or concerns in relation to its service or approach?



Answer Choices	Responses	
We have found the ICO to be responsive to discussion and flexible in its approach	11	73.33%
We have found the ICO to be partially responsive to discussion and flexible when required	2	13.33%
We have found the ICO to be slow to respond when contracted or inflexible in its approach	2	13.33%
We have found it difficult to enter into meaningful discussion or not found the approach to be at all collaborative	0	0.00%
<b>Total</b>	<b>15</b>	<b>100%</b>



## Q14 Are you able to expand upon your previous answer?

### Detailed Responses

- “The ICO has always extended a deadline when requested.”
- “There is a willingness to work together and to take a pragmatic/proportionate approach.”
- “The Council has been under a period of performance monitoring by the ICO this year, and was visited by the Commissioner’s Office in July. We experienced some difficulty in arranging a date to meet, and indeed, an initial arrangement for our staff to visit the Commissioner’s offices in Manchester was cancelled by the ICO at very short notice. In addition, we have found that some investigations in data protection concerns are extremely prolonged (12 months and above), which results in significant uncertainty for the council, as the threat of significant fines is left ‘hanging over’ us, with the added risk that any subsequent breach may be ‘counted towards’ the original sanction. In the interests of balance, the Council does note that the ICO has, on occasion, clearly appreciated the difficulties being experienced by the Council, and has responded in an appropriately flexible way. A dedicated contact point for organisations like Local Government, where staff could ask for advice without fear of punitive action would build confidence in the ICO’s commitment to working with agencies to improve information governance standards.”
- “ICO has been slow to respond to correspondence in a number of different cases and appeared defensive in cases where we have stated that it would have been preferable to consult us before deciding that we had likely breached DP principles.”
- “The responses we obtain from the Policy Team are pragmatic and helpful. The team is open to detailed discussion and consistently provides feedback and suggestions to help our business.”
- “The only comment that I would make is that when we issue one point of contact this is ignored and communications continues to be received via numerous officers.”
- “The times for a response requested by the ICO are often unachievable given the size of our organisation. The ICO has been flexible around when responses are required.”
- “We have a great relationship with the team handling complaints, including quarterly meetings to review cases and ad hoc phone conversations to resolve cases more quickly. The current regime is really working for us. We just disagree with the publication of data on the basis that you are using at the present time.”

## B Internal Audit Approach

### Approach

Our role as internal auditor to a Public Body is to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance processes, by measuring and evaluating their effectiveness in achieving the organisation's agreed strategic objectives.

The 2015-16 Audit plan included a review of core operations, in particular how the ICO handles enquiries, written concerns and complaints from the general public and organisations.

Following the implementation of operational changes made by Project Eagle, it was agreed with management that the ICO would obtain greater value from revisiting the results of the 2013-14 ICO consultation entitled, "Our new approach to data protection concerns" to provide an objective appraisal of the changes made.

We achieved this by:

- Engaging with the respondents to the original consultation document, using a questionnaire agreed with ICO management, to understand what impact operational changes had on their organisations (if any), and how the ICO has worked with them to improve their information rights practices since implementation;
- Engaging with a further sample of organisations with which the ICO has engaged, from complaints, regulatory action or voluntary review to understand the effectiveness of the engagement, again using a questionnaire to be agreed with ICO management; and

- Confirmed that the ICO has published information, by organisation and sector, relating to concerns received together with consultation documents and legislative guides that align with Corporate Plan deliverables and the changing external environment.

### Responsibilities

The Information Commissioner acts through his Board of Management and the Information Commissioner's Office ("ICO") discharges his obligations. Therefore, references to the Information Commissioner and the ICO in this report relate to one and the same party.

It is the responsibility of the Information Commissioner to ensure that the ICO has adequate and effective risk management, control and governance processes.

HM Treasury's Corporate Governance in Central Government Departments (2011) states that boards of Public Bodies should determine the nature and extent of the significant risks it is willing to take in achieving its strategic objectives. The Board should therefore maintain sound risk management and internal control systems and should establish formal and transparent arrangements for considering how they should apply the corporate reporting and risk management and internal control principles and for maintaining an appropriate relationship with the organisation's auditors.

Please refer to our letter of engagement for full details of responsibilities and other terms and conditions.

---

## Scope

Our review involved an assessment of the following risks:

- The ICO's updated approach to engagement and consultation significantly increases the burden of activity for external organisations, resulting in these organisations being unable to effectively manage engagements, develop effective data management governance or mitigate thematic problems identified;
- The ICO may not undertake investigations that are proportional to the potential severity of the matters involved resulting in organisations receiving recommendations which are not seen as being effective by the organisations and hence are not being implemented; and
- The ICO does not publish complete or meaningful information on the outcomes of its regulatory work or provide an effective regulatory view on the risks and threats to compliance in each sector and any plans for future improvements.

## Additional information

### Client staff

The following staff were consulted as part of this review:

- Paul Arnold (Head of Customer and Business Services);
- Andy Laing (Head of Performance Improvement).

### Documents received

The following documents were received during the course of this audit:

- Original consultation approach (January 2014);
- Responses to consultation;
- Detailed consultation responses.

### Locations

We visited The Information Commissioner's Office, Wilmslow during the scoping of our work, and completed fieldwork remotely.



© 2016 Grant Thornton UK LLP. All rights reserved

“Grant Thornton” refers to the brand under which the Grant Thornton member firms provide assurance, tax and advisory services to their clients and/or refers to one or more member firms, as the context requires.

Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. GTIL and each member firm is a separate legal entity. Services are delivered by the member firms. GTIL does not provide services to clients. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

**[grant-thornton.co.uk](http://grant-thornton.co.uk)**